



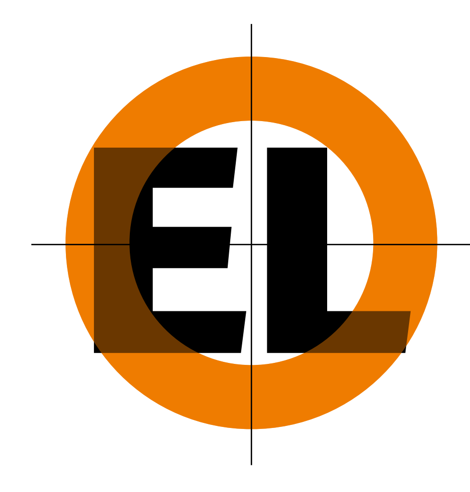
Puede que pronto escuadrillas de aeronaves no tripuladas surquen los cielos con fines civiles. Sin embargo, varios fallos de seguridad permiten secuestrarlas con técnicas simples

Kyle Wesson y Todd Humphreys

DAN WINTERS

Kyle Wesson es estudiante de doctorado en ingeniería eléctrica e informática en la Universidad de Texas en Austin. Pertenece al Grupo de Comunicaciones y Redes Inalámbricas del Laboratorio de Radionavegacion, donde desarrolla técnicas afines al sistema GPS.

Todd Humphreys es profesor de ingeniería aeroespacial en la Universidad de Texas en Austin. Dirige el Laboratorio de Radionavegación, donde investiga técnicas de navegación por satélite.



2 DE AGOSTO DE 2010, UN HELICÓPTERO DE LA MARINA ESTADOUNIDENSE sobrevolaba perezosamente el restringido espacio aéreo que se extiende sobre la capital del país. El acontecimiento podría no haber pasado de una anotación rutinaria en los registros de tráfico aéreo del Aeropuerto Nacional Ronald Reagan, de no ser por un detalle inquietante: en el aparato no viajaba nadie. Carecía de ventanas y su cabina solo contenía instrumentación electrónica. Era un vehículo aéreo no tripulado (VANT) o, más conocido ahora, dron (de *drone*, «zángano» en inglés).

El Fire Scout MQ-8B, de 1429 kilogramos y 9,7 metros de largo, había sufrido lo que los encargados de investigar el caso llamarían después un «problema de programación»: una caída de las comunicaciones con el equipo de operadores que, impotentes, permanecían en una sala de control de la estación aeronaval de Patuxent River, en el estado de Maryland. Para empeorar las cosas, el dron incumplió las instrucciones preprogramadas que, en una situación así, debían hacer que regresara a la base. El Fire Scout, destinado al reconocimiento de buques de guerra, había invadido el mismo espacio aéreo que usa el *Air Force One* (el avión oficial del presidente de EE.UU.) en sus despegues y aterrizajes.

Tras media hora de nerviosismo, los operadores lograron restablecer la comunicación y recuperaron el control del objeto. Más tarde, un alto cargo de la Marina trataría de resaltar el lado bueno del incidente subrayando el buen comportamiento de la aeronave durante aquel desvío inesperado. El sistema de pilotaje automático, por ejemplo, la mantuvo volando en línea recta y en un mismo plano.

El caso del Fire Scout ilustra con claridad los enormes problemas de seguridad que aún plantean los vehículos aéreos no tripulados. Estos emblemáticos aparatos militares ya están comenzando a usarse para toda clase de tareas civiles. La Administración Federal de la Aviación estadounidense (FAA) estima que, hacia 2020, más de 10.000 VANT sobrevolarán el país. Muy pronto podrán dedicarse a labores de rescate, fumigación de cultivos, vigilancia de líneas eléctricas, investigaciones científicas y numerosas tareas más.

Los argumentos para emplear drones suenan convincentes. Prescindir del piloto y de todo el equipo necesario para acomodar a la tripulación y los pasajeros supondría un enorme ahorro en las operaciones aéreas comerciales. Por el mismo precio que cuesta alquilar un avión pilotado para llevar a cabo varias inspecciones de la red eléctrica, una empresa podría adquirir una nave no tripulada que realizaría la misma tarea durante años. El atractivo de los drones ha cautivado a las mayores empresas de transporte estadounidenses. Frederick W. Smith, fundador y presidente de FedEx, habla ya de sustituir por aeronaves no tripuladas su flota entera de distribución aérea.

También el Congreso de EE.UU. es consciente de que el país se acerca a la era de los VANT comerciales. Cuando en febrero de 2012 se aprobó la Ley de Modernización y Reforma de la FAA, la cámara ordenó a la agencia que redactara un plan completo para acelerar, de manera segura, la integración de sistemas aéreos civiles no tripulados en el espacio aéreo del país. Dicho informe debería estar terminado para 2015.

Por desgracia, no parece probable que la legislación necesaria para regular el vuelo de drones —en esencia, robots por control remoto— vaya a estar lista a tiempo. Las aeronaves no tripuladas exigen ampliar la responsabilidad de la FAA más allá de lo que

EN SÍNTESIS

Se prevé que, hacia 2020, más de 10.000 aeronaves no tripuladas surquen los cielos de EE.UU. en labores de vigilancia y rescate, control de redes eléctricas y otras tareas debido al ahorro que supondrá prescindir de los pilotos.

El uso de estos vehículos plantea toda clase de problemas de seguridad para las que los organismos reguladores aún no están preparados. Sus cometidos tradicionales deberán ampliarse para impedir el secuestro de las aeronaves y otros percances.

Será necesario desarrollar medios técnicos que garanticen la estabilidad de las comunicaciones con tierra. Las nuevas regulaciones también deberán afrontar otras cuestiones, como las relacionadas con la privacidad.

PUNTOS DÉBILES

Maneras de engañar a un dron

Los fallos de seguridad en las transmisiones de control pueden aprovecharse para secuestrar la aeronave. El envío de señales falsas o el bloqueo de las legítimas puede hacer que esta se desvíe de su trayectoria y se estrelle. Los expertos en seguridad han demostrado que es posible llevar a cabo varios tipos de ataque, ilustrados aquí con un modelo Schiebel Camcopter.

Satélites GPS

Transmisión de señales de navegación

Señales del transpondedor

Transmisiones de suplantación y bloqueo

Desde tierra, un operador guía la aeronave mediante señales de radio que pueden ser interferidas.

Señales de control

Las transmisiones de un transpondedor, que advierten a otros vuelos de la cercanía de la aeronave, pueden ser suplantadas o bloqueadas.

Señales suplantadoras

Interferencias

Interferencia
La transmisión de señales de ruido puede bloquear la navegación y otras comunicaciones clave. Aunque es posible programar una aeronave para que regrese a la base si pierde las señales de control, no se conoce ninguna solución satisfactoria en caso de que fallen al mismo tiempo las transmisiones de la base y la recepción de señales GPS.

GPS SCRAMBLED

Suplantación (*spoofing*)
Un controlador electrónico puede falsificar las señales procedentes de los satélites GPS o de los transpondedores de un avión cercano. Las señales simuladas pueden ser más intensas que las legítimas, lo que haría que el dron se desviase de su ruta y se aproximase en exceso a otra aeronave. Una solución consistiría en cifrar las comunicaciones mediante una firma digital reconocible, pero el desarrollo de una técnica semejante aún tardará años en llegar. Por el momento, no se conocen alternativas fiables.

hasta ahora han sido sus cometidos tradicionales, como asegurar que dos Boeing 747 no se acerquen demasiado uno a otro o que no sufran las inclemencias meteorológicas. Aunque después de los atentados del 11-S la misión de la agencia se haya ampliado para garantizar ciertos aspectos de la seguridad de los vehículos aéreos (fue la FAA la encargada de supervisar la instalación de puertas reforzadas en las cabinas de pilotaje), la perspectiva de gestionar bandadas de drones plantea más problemas que los que la agencia puede afrontar.

ENLACES VITALES

El más sobrecogedor de todos esos desafíos consiste en asegurar las conexiones del aparato con el exterior. Maniobrar un VANT requiere disponer de tres enlaces de comunicación principales: la señal entrante de los satélites GPS; uno o varios vínculos que notifiquen a otras aeronaves los movimientos del vehículo; y una conexión bidireccional con la base terrestre que permita a los operadores pilotar la nave. La interrupción de cualquiera de esos enlaces puede provocar un desastre. Sin embargo, existen casos para los que no se conoce ninguna técnica clara que garantice su seguridad.

El GPS constituye la pieza clave del sistema de navegación de un dron. Complementa a los sensores de guía inercial, los magnetómetros, los altímetros e incluso las cámaras. El receptor GPS ocupa un lugar privilegiado entre todos ellos porque, a diferencia de los demás instrumentos, funciona bajo cualquier condición meteorológica sin comprometer nunca su enorme precisión. Pero, al contrario que la versión militar, el GPS civil es de libre acceso

BROWN BIRD DESIGN

y no está cifrado. Usado hoy en teléfonos inteligentes o relojes deportivos, carece de cualquier tipo de autenticación, lo que conlleva el riesgo de que su señal sea sustituida por una falsa. Este tipo de ataque se conoce como suplantación (*spoofing*).

En junio de 2012, en la zona de prueba de misiles de White Sands, en Nuevo México, nuestro laboratorio demostró que la vulnerabilidad que presenta el sistema GPS a la suplantación entraña graves consecuencias para los vehículos aéreos no tripulados. A medio kilómetro de distancia, nuestro dispositivo tomó el control de un dron de 80.000 dólares. Nuestro aparato, fabricado a mano, emuló casi a la perfección las señales de satélite que transmiten las coordenadas al dron. Al no poder distinguir las señales verdaderas de las falsas, la nave se guió por las nuestras, más intensas.

Una vez engañado, el dron interpretaba las señales de nuestro artilugio como órdenes de posicionamiento. Si estas indicaban —falsamente— que la nave estaba ascendiendo, el aparato bajaba para mantener la altitud programada en su sistema de autopilotaje. Al tratar de ajustar su posición basándose en datos erróneos, el dron comenzó a dirigirse en línea recta contra el suelo. Solo lo salvó de la catástrofe un operador preparado para desoír las instrucciones falsas y hacerse manualmente con el control de la nave.

Los riesgos que entraña la suplantación se conocen desde hace una década. Un informe del Departamento de Transporte de EE.UU. ya avisó de sus peligros en 2001. Sin embargo, los legisladores y los fabricantes de sistemas GPS apenas lo tomaron en consideración hasta hace muy poco, tal vez confiados en que un ataque de ese estilo resultaba demasiado improbable para merecer atención. Pero las soluciones técnicas no se antojan fáciles. Los métodos para proteger las señales GPS mediante marcas de agua criptográficas (firmas digitales seguras que certifican la procedencia de un mensaje y garantizan su contenido) tardarán años en implementarse. Y otras alternativas no criptográficas que sí cabría poner en marcha en menos tiempo deben aún demostrar su validez.

Pero la suplantación del sistema GPS no es la única amenaza que se cierne sobre los VANT. Bloquear su recepción también resulta sorprendentemente sencillo. Cerca de la superficie terrestre, sus señales se muestran muy tenues: su densidad de flujo (una medida de la intensidad) no supera a la de una bombilla de 50 vatios situada a 22.000 kilómetros de distancia. Un dispositivo que pretenda interferirlas no tendría más que enviar una señal ruidosa en la misma región del espectro que emplean los sistemas GPS. Y casi cualquier aparato electrónico moderno, ordenadores portátiles incluidos, podría interferir de manera involuntaria la señal del GPS si se encuentra lo suficientemente cerca de la aeronave.

Un dispositivo diseñado ex profeso para provocar interferencias puede llegar a resultar muy eficaz a la hora de alterar el sistema de navegación de una aeronave no tripulada. En mayo de 2012, en Corea del Sur, los operadores perdieron el control de un Schiebel Camcopter S-100, un VANT de reconocimiento de 150 kilogramos que acabó estrellándose contra la base de operaciones. El accidente mató a un ingeniero e hirió a dos técnicos. Lo más probable es que la secuencia de acontecimientos que condujeron a la catástrofe se precipitase por efecto de interferencias procedentes de Corea del Norte, a las que se sumaron varios errores humanos por parte de los operadores del vehículo. Estos casos ponen de manifiesto que una navegación segura, resistente a la suplantación y a las interferencias, resultará esencial si deseamos asegurar un tráfico seguro de aeronaves no tripuladas.

Un informe reciente reconocía que, por el momento, no se han desarrollado los medios técnicos necesarios para dotar a los drones de un sistema que impida las colisiones

PREVENIR LOS CHOQUES

La posibilidad de que un VANT colisione en pleno vuelo con otra aeronave complicará aún más su aceptación. En los aviones tradicionales, los pilotos se valen del radar y de su sentido de la vista para detectar la presencia de aviones cercanos. Sin embargo, a los drones aún les queda un largo camino por recorrer antes de alcanzar ese nivel de vigilancia. En un informe de 2012, la Oficina de Evaluación Gubernamental de EE.UU. reconocía que, por el momento, no se han desarrollado los medios técnicos necesarios para dotar a las aeronaves no tripuladas de un sistema antichoque que, al mismo tiempo, respete las normas de la FAA.

No interponerse en el camino de otra aeronave resulta especialmente difícil para los VANT de menor tamaño. Estos no pueden transportar los equipos de radar actuales, pues resultan muy voluminosos y consumen grandes cantidades de energía. Y aunque las cámaras de luz visible e infrarrojos aportan una solución asequible y de eficacia razonable, no pueden detectar objetos detrás de las nubes.

En último término, la solución podría venir de los sistemas de vigilancia dependiente automática por transmisión (ADS-B, por sus siglas en inglés). Un transpondedor ADS-B comunica cada segundo la posición y velocidad de la aeronave, al tiempo que recibe informes similares de los aparatos que se encuentran cerca. Para 2020, en el marco de una gran revisión del sistema de tráfico aéreo de EE.UU., la FAA exigirá que todas las aeronaves, grandes o pequeñas, lleven transpondedores ADS-B. Siempre que un conjunto de naves próximas —tripuladas o no— se comuniquen su posición mediante ADS-B, las colisiones podrían evitarse.

Pero, como ocurre con el GPS civil, también el ADS-B tiene su talón de Aquiles. Sus transmisiones no están autenticadas, por lo que se prestan a la falsificación. Cuando comenzó a desarrollarse el ADS-B, en los años noventa, la seguridad no representaba un problema: la idea de transmitir señales falsas era casi inconcebible. Sin embargo, los requisitos técnicos y los conocimientos necesarios para provocar un ataque han disminuido de modo alarmante desde entonces. En 2012, los investigadores del Instituto de Tecnología de la Fuerza Aérea de EE.UU. demostraron que era posible llevar a cabo toda una serie de ataques mediante señales falsas. Estas podían codificarse y transmitirse desde tierra o aire, sin más que usar una antena sencilla. Tales «in-

yecciones falsas» pueden hacer creer al sistema de navegación de un VANT que una colisión es inminente.

Por otro lado, las mismas técnicas permiten generar cientos de transmisiones falsas o bloquear la recepción de mensajes legítimos. Los mensajes de ADS-B adulterados plantearían mayores problemas a los drones pequeños que a los aviones tripulados. En estos últimos, el radar de abordo alerta al piloto, que puede verificar con rapidez si se aproxima otra aeronave o no. Un VANT, en cambio, carece de un sistema de alerta semejante.

La FAA pretende eludir el riesgo de los falsos mensajes de ADS-B por medio de sistemas de multilateración: una técnica que localiza el origen de una señal a partir de los tiempos relativos de llegada a varios receptores terrestres para, después, transmitir esa información a un avión en vuelo. No obstante, un sistema de multilateración fiable requiere una alternativa precisa al GPS; sin embargo, aún no existe ninguna versión asequible.

Por último, el control de los VANT se realiza a través de una conexión inalámbrica entre el operador y la nave. A primera vista, ello parece plantear menos problemas de seguridad que el sistema GPS o el ADS-B, ya que existen protocolos de comunicación seguros que lo protegen de la suplantación u otros ataques. Sin embargo, aún resulta posible bloquear las señales. La pérdida de contacto con el dron (lo que los expertos llaman la «caída del enlace») puede ser provocada tanto por interferencias intencionadas como por un fallo de funcionamiento, problemas para los que aún no se conocen soluciones satisfactorias. Los operadores suelen configurar los drones con protocolos que, por ejemplo, ordenen a la nave regresar a la base si la conexión se pierde durante más de 30 segundos. Sin embargo, tales métodos dependen de que el sistema de navegación del dron —en sí vulnerable a ataques externos— funcione correctamente y de que los dispositivos de control no sufran fallos informáticos, como ocurrió con el Fire Scout de Washington.

Otro problema al que se enfrentan los reguladores es el de asignar bandas de radio exclusivas a la transmisión de señales de control. Debido a la escasez del espectro disponible, no pocos drones se verán obligados a recurrir a frecuencias no protegidas, empleadas en otro tipo de comunicaciones. En tal caso, las señales podrían verse afectadas por las interferencias involuntarias que provocasen los dispositivos que ya operan en dichas bandas.

EL PROBLEMA DE LA REGULACIÓN LEGAL

En EE.UU., a la complejidad técnica de lograr VANT seguros se suma una burocracia lenta y reacia a asumir riesgos, así como una creciente ofuscación legislativa. Los reguladores deben aceptar que existe una nueva manera de gobernar una aeronave. El operador que maneja un VANT no es un piloto que empuña los mandos sin apartar la vista del parabrisas. En su lugar, ha de introducir la ruta de vuelo en un ordenador, controlar el vehículo con una palanca y monitorizar el estado de varios enlaces de comunicaciones. Durante un vuelo, habrá ocasiones en las que el operador manejará el dron como si se tratase de un avión de miles de kilogramos dirigido por control remoto; en otras, puede que la nave vuele por sí sola con total autonomía.

La FAA tiene a su cargo garantizar que el sistema de tráfico aéreo del EE.UU. consiga los recursos técnicos necesarios para que un dron pueda compartir con seguridad el mismo espacio aéreo que un Airbus 380 o un monomotor Piper Mirage. Por tanto, la agencia deberá aprobar regulaciones que impidan que la pérdida de las comunicaciones con el dron suponga una amenaza.

El brillante historial de la FAA en materia de seguridad se debe, en parte, a su precaución a la hora de adoptar nuevas técnicas que pudieran perturbar el tráfico aéreo. Ahora, la agencia debe hacer frente a la compleja cuestión de reglamentar el tráfico de drones al mismo tiempo que lleva a cabo una vasta modernización del sistema aéreo estadounidense: el Sistema de Transporte Aéreo de la Siguiente Generación o NextGen, que pretende sustituir los radares por sistemas de navegación basados en comunicaciones por satélite. En teoría, el Departamento de Seguridad Nacional debería prestar ayuda, pero sus responsables han repetido en varias ocasiones que los VANT no forman parte de sus competencias.

Al elaborar las regulaciones, la FAA tendrá que encontrar un difícil equilibrio entre la seguridad pública y los beneficios económicos que conlleva el uso de drones. Exigir que una aeronave no tripulada se mantenga siempre al alcance de la vista del operador reduciría las posibilidades de secuestro, pero haría de estos vehículos un recurso inútil para multitud de propósitos. El uso de aeronaves no tripuladas plantea, asimismo, cuestiones de privacidad que, en el pasado, la FAA jamás se ha visto obligada a considerar. Tanto los grupos que velan por garantizar los derechos de privacidad como varios parlamentarios han reclamado ya a la agencia que dicte normas que hagan frente a la posibilidad de que un dron provisto de una cámara de alta definición sobrevuele patios suburbanos.

Entre tanto, numerosos legisladores no ven con buenos ojos la introducción de drones, artefactos a los que se han acostumbrado a ver en los telediarios vigilando y bombardeando zonas de conflicto en otros países. Al menos 42 estados han propuesto límites legales a su uso. Una ley aprobada recientemente en Texas tipifica como infracción que una aeronave no tripulada tome imágenes de una propiedad privada sin el consentimiento expreso del dueño. A nivel estatal, una iniciativa legislativa de 2013 ha propuesto prohibir que los cuerpos policiales empleen drones en labores de vigilancia sin una orden judicial. El mismo proyecto también vetaba el uso de drones equipados con armamento, tanto por parte de civiles como por parte de las fuerzas de seguridad.

Parece probable que esa lista de requisitos técnicos y normativos, así como todas las preocupaciones expresadas por los legisladores, retrasen la adopción de VANT para usos civiles, pero no que la detengan. Las cuestiones de seguridad que conllevan deben analizarse con cierta perspectiva. Muchas de sus vulnerabilidades son análogas a las que desde hace tiempo afectan a los vuelos pilotados: un avión también puede ser secuestrado, su tripulación puede sufrir coacciones y la comunicación con tierra puede perderse. Con todo, continuamos volando. Y no porque ignoremos tales riesgos, sino porque los beneficios del tráfico aéreo superan con creces los inconvenientes. Al final, los drones exigirán de nosotros una concesión similar.

PARA SABER MÁS

Unmanned aircraft systems: Measuring progress and addressing potential privacy concerns would facilitate integration into the national airspace system. Oficina de Evaluación Gubernamental de EE.UU., 18 de septiembre de 2012. Disponible en **www.gao.gov/products/GAO-12-981**

Unmanned at any speed: Bringing drones into our national airspace. Wells C. Bennet. Issues in Governance Studies series, n.º 55. Brooking Institution, 14 de diciembre de 2012. Disponible en **www.brookings.edu/research/papers/2012/12/14-drones-bennett**

INVESTIGACIÓN Y CIENCIA

Abril 2014, Número 451

32

ARTÍCULOS

